[COMMITTEE PRINT]

June 22, 2004

[Showing H.R. 2929, As Adopted by the Subcommittee on Commerce, Trade, and Consumer Protection]

108TH CONGRESS
1ST SESSION

H. R. 2929

To protect users of the Internet from unknowing transmission of their personally identifiable information through spyware programs, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JULY 25, 2003

Mrs. BONO (for herself and Mr. TOWNS) introduced the following bill; which was referred to the Committee on Energy and Commerce

[Strike out all after the enacting clause and insert in lieu thereof the part printed in roman]

[For text of introduced bill, see copy of bill as introduced on July 25, 2003]

A BILL

To protect users of the Internet from unknowing transmission of their personally identifiable information through spyware programs, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Securely Protect Yourself Against Cyber Trespass Act'' or the ''SPY ACT''.

SEC. 2. PROHIBITION OF DECEPTIVE ACTS OR PRACTICES RELATING TO SPYWARE.

(a) PROHIBITION.—It is unlawful for any person, who is not the owner or authorized user of a protected computer, to engage in deceptive acts or practices in connection with any of the following conduct with respect to the protected computer:

(1) Taking control of the computer, including—

(A) utilizing such computer or computing services to send unsolicited information or material to others;

(B) diverting the Internet browser of the computer, or similar program of the computer used to access and navigate the Internet, to one or more Web pages not of the owner or authorized user's choosing;

(C) accessing or using the modem, or Internet connection or service, for the computer and thereby causing damage to the computer or causing the owner or authorized user to incur unauthorized financial charges;

(D) using the computer as part of an activity performed by a group of computers that cause damages to another computer; and

(E) delivering advertisements that a user of the computer cannot close without turning off the computer or closing all sessions of the Internet browser for the computer.

(2) Modifying settings related to the computer's access to or use of the Internet, including by altering—

(A) the Web page that appears when the owner or authorized user launches an Internet browser or similar program used to access and navigate the Internet;

(B) the default provider used to access or search the Internet, or other existing Internet connections settings;

(C) a list of bookmarks used by the computer to access Web pages; or

(D) security or other settings of the computer that protect information about the owner or authorized user.

(3) Collecting personally identifiable information through the use of a keystroke logging function

or similar function and transferring such information from the computer to another person.

(4) Monitoring, or analyzing the content of, the Web pages or other online locations accessed using the computer.

(5) Inducing the owner or authorized user to install a computer software component onto the computer, or preventing reasonable efforts to block the installation or execution of, or to disable, a computer software component, including by—

(A) presenting the owner or authorized user with an option to decline installation of a software component such that, when the option is selected by the owner or authorized user, the installation nevertheless proceeds; or

(B) causing a computer software component that the owner or authorized user has removed or disabled to automatically reinstall or reactivate on the computer.

(6) Representing that installing a separate software component or providing log-in and password information is necessary for security or privacy reasons, or that installing a separate software component is necessary to open, view, or play a particular type of content.

(7) Installing or executing computer software on the computer, without the permission of the party named as the provider of the software, to deceive the owner or authorized user about the identity of the person or service responsible for the functions performed or the content displayed by such computer software.

(8) Installing or executing on the computer one or more additional computer software components with the intent of causing a person to use such components in a way that violates any other provision of this section.

(9) Removing, disabling, or rendering inoperative a security, anti-spyware, or anti-virus technology for the computer.

(b) EFFECTIVE DATE.—This section shall take effect on the date of the enactment of this Act.

SEC. 3. PROHIBITION OF COLLECTION OF CERTAIN INFORMATION WITHOUT NOTICE AND CONSENT.

(a) OPT-IN REQUIREMENT.—Except as provided in subsection (e), it is unlawful for any person—

(1) to transmit to a protected computer, which is not owned by such person and for which such person is not an authorized user, any information collection program, or

(2) to enable the operation of any information collection program with respect to such a protected computer,

unless, before such transmission or enabling, the owner or an authorized user of the protected computer has consented to such transmission or enabling pursuant to notice in accordance with subsection (c) and such information collection program includes the functions required under subsection (d).

(b) INFORMATION COLLECTION PROGRAM.—For purposes of this section, the term ''information collection program'' means computer software that—

(1)(A) collects personally identifiable information; and

(B)(i) sends such information to a person other than the owner or authorized user of the computer, or (ii) uses such information to deliver advertising to, or display advertising, on the computer; or

(2)(A) collects information regarding the Web pages accessed using the computer; and

(B) uses such information to deliver advertising to, or display advertising on, the computer.

(c) NOTICE AND CONSENT.—

(1) IN GENERAL.—Notice in accordance with this subsection with respect to an information collec-

tion program is clear and conspicuous notice in plain English, set forth in a form and manner as the Commission shall provide, that—

(A) clearly distinguishes such notice from any other information visually presented contemporaneously on the protected computer;

(B) states as follows: ''This program will collect and transmit information about you and your computer use. Do you accept?'';

(C) provides for the user to grant or deny consent referred to in subsection (a) by selecting a ''Yes'' or ''No'' option;

(D) provides an option for the user to select to display on the computer, before granting or denying consent using the option required under subparagraph (C), a clear description of—

(i) the types of information to be collected and sent (if any) by the information collection program; and

(ii) the purpose for which such information is to be collected and sent.

(E) provides for concurrent display of the information required under subparagraphs (B) and (C) and the option required under subpara-

graph (D) until the user grants or denies consent using the option required under subparagraph (C) (or selects the option required under subparagraph (D)).

(2) CHANGE IN INFORMATION COLLECTED.—The Commission shall provide that the owner or authorized user of a protected computer shall not be considered to have consented to transmission to, or enabling with respect to, the protected computer of an information collection program for purposes of subsection (a) if after granting consent pursuant to a notice in accordance with this subsection—

(A) the description required under paragraph (1)(D) to be included in the notice does not include—

(i) information of a type that the program collects or sends; or

(ii) a purpose for which such information is collected or sent; and

(B) the owner has not previously been provided further notice in accordance with this subsection that includes, in such description, such type of information or purpose for collection or sending, respectively.

(3) REGULATIONS.—The Commission shall issue regulations to carry out this subsection.

(d) REQUIRED FUNCTIONS.—The functions required under this subsection to be included in an information collection program transmitted to, or enabled with respect to, a protected computer are as follows:

(1) DISABLING FUNCTION.—With respect to each information collection program, a function of the program, as the Commission shall, by regulation provide, that allows a user of the program to remove the program or disable operation of the program with respect to such protected computer by a function that—

(A) is easily identifiable to a user of the computer; and

(B) can be performed without undue effort or knowledge by the user of the protected computer.

(2) IDENTITY FUNCTION.—With respect only to an information collection program that uses information collected in the manner described in paragraph (1)(B)(ii) or (2)(B) of subsection (b), a function of the program that provides that each display of an advertisement directed or displayed using such infor-

mation is accompanied by a statement that clearly identifies the information collection program.

(e) LAW ENFORCEMENT AUTHORITY.—Subsection (a) shall not apply in the case of the transmission or enabling of an information collection program in compliance with a law enforcement, investigatory, national security, or regulatory agency or department of the United States in response to a request or demand made under authority granted to that agency or department, including a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a court order, or a compulsory administrative process.

(f) LIMITATION ON LIABILITY.—A telecommunications carrier (as such term is defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153), information service provider (as such term is defined in such section), or other provider of underlying transmission capability shall not be liable under this section solely because—

(1) the carrier or provider transmitted, routed, stored, or provided connections for an information collection program through a system or network controlled or operated by or for the carrier or provider; or

(2) of the intermediate and transient storage of such a program in the course of such transmission, routing, storing, or provision of connections.

SEC. 4. ENFORCEMENT.

(a) UNFAIR OR DECEPTIVE ACT OR PRACTICE.—This Act shall be enforced by the Commission under the Federal Trade Commission Act (15 U.S.C. 41 et seq.). A violation of any provision of this Act or of a regulation issued under this Act shall be treated as an unfair or deceptive act or practice violating a rule promulgated under section 18 of the Federal Trade Commission Act (15 U.S.C. 57a), except that the maximum civil penalty for a violation of this Act shall be one of the following amounts, as the Commission, in its discretion, applies to such a violation:

(1) $33,000 for each violation, except that in applying this subparagraph each separate protected computer to which an information collection program is transmitted, or with respect to which such a program is enabled, in violation of this Act shall be treated as a separate violation.

(2) In the case of a violation of—

(A) section 2(a), $3,000,000; and

(B) section 3(a), $1,000,000, except that in applying this subparagraph in the case of

violation of this Act involving transmitting an information collection program to protected computers, a single transmission directed to multiple protected computers shall be treated as a single violation regardless of the number of protected computers to which such transmission is made.

(b) ACTIONS BY FTC.—The Commission shall prevent any person from violating this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act. Any entity that violates any provision of this Act is subject to the penalties (except as modified by subsection (a)) and entitled to the privileges and immunities provided in the Federal Trade Commission Act in the same manner, by the same means, and with the same jurisdiction, power, and duties as though all applicable terms and provisions of the Federal Trade Commission Act were incorporated into and made a part of this Act.

(c) EXCLUSIVENESS OF REMEDIES.—The remedies in this section are the exclusive remedies for violations of this Act.

(d) EFFECTIVE DATE.—This section shall take effect on the date of the enactment of this Act, but only to the extent that this section applies to violations of section 2(a).

SEC. 5. EFFECT ON OTHER LAWS.

(a) PREEMPTION OF STATE LAW.—

(1) PREEMPTION.—This Act supersedes any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates—

(A) deceptive or misrepresentative conduct with respect to computers similar to that described in section 2(a); or

(B) the transmission or enabling of a computer program similar to that described in section 3.

(2) PROTECTION OF CERTAIN STATE LAWS.—This Act shall not be construed to preempt the applicability of—

(A) State trespass, contract, or tort law; or

(B) other State laws to the extent that those laws relate to acts of fraud.

(b) PRESERVATION OF FTC AUTHORITY.—Nothing in this Act may be construed in any way to limit or affect the Commission's authority under any other provision of law.

SEC. 6. ANNUAL FTC REPORT.

For the 12-month period that begins upon the effective date under section 9(a) and for each 12-month period thereafter, the Commission shall submit a report to the Congress that—

(1) specifies the number and types of actions taken during such period to enforce sections 2(a) and 3, the disposition of each such action, any penalties levied in connection with such actions, and any penalties collected in connection with such actions; and

(2) describes the administrative structure and personnel and other resources committed by the Commission for enforcement of this Act during such period.

Each report under this subsection for a 12-month period shall be submitted not later than 90 days after the expiration of such period.

SEC. 7. REGULATIONS.

Any regulations issued pursuant to this Act shall be issued in accordance with section 553 of title 5, United States Code.

SEC. 8. DEFINITIONS.

For purposes of this Act:

(1) COMPUTER; PROTECTED COMPUTER.—The terms ''computer'' and ''protected computer'' have

the meanings given such terms in section 1030(e) of title 18, United States Code.

(2) COMPUTER SOFTWARE.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the term ''computer software'' means a set of statements or instructions to be used directly or indirectly by a computer to bring about a certain result.

(B) EXCEPTION FOR COOKIES.—Such term does not include a cookie, or other text file, placed on the computer system of a user by an Internet service provider, interactive computer service, or Internet website to return information to the Internet service provider, interactive computer service, Internet website, or third party if the user subsequently uses the Internet service provider or interactive computer service, or accesses the Internet website.

(3) COMMISSION.—The term ''Commission'' means the Federal Trade Commission.

(4) DAMAGE.—The term ''damage'' has the meaning given such term in section 1030(e) of title 18, United States Code.

(5) DECEPTIVE ACTS OR PRACTICES.—The term ''deceptive acts or practices'' has the meaning

applicable to such term for purposes of section 5 of the Federal Trade Commission Act (15 U.S.C. 45).

(6) DISABLE.—The term 'disable' means, with respect to an information collection program, to permanently prevent such program from executing any of the functions described in section 3(b) that such program is otherwise capable of executing, unless the owner or operator of a protected computer takes a subsequent affirmative action to enable the execution of such functions.

(7) ENABLE.—The term ''enable'' means, with respect to an information collection program, to take such actions as are necessary to make the program operational with respect to carrying out the functions described in section 3(b) that the program is capable of executing.

(8) INTERNET.—The term ''Internet'' means collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire or radio.

(9) PERSONALLY IDENTIFIABLE INFORMATION.—

(A) IN GENERAL.—The term ''personally identifiable information'' means:

(i) First and last name of an individual.

(ii) A home or other physical address of an individual, including street name, name of a city or town, and zip code, but not including solely the name of a city or town or a zip code, individually or together.

(iii) An electronic mail address.

(iv) A telephone number.

(v) A social security number, tax identification number, passport number, driver's license number, or any other government-issued identification number.

(vi) A credit card number.

(vii) An account number.

(viii) Any access code or password, other than an access code or password that is transferred by an owner or authorized user of a protected computer to the intended third party.

(ix) Date of birth, birth certificate number, or place of birth of an individual, except in the case of a date of birth required by law to be transmitted or collected.

(B) RULEMAKING.—The Commission may, by regulation, add to the types of information specified under paragraph (1) that shall be considered personally identifiable information for purposes of this Act, except that such information may not include any record of aggregate data that does not identify particular persons, particular computers, particular users of computers, or particular email addresses or other locations of computers with respect to the Internet.

(10) TRANSMIT.—The term ''transmit'' means, with respect to an information collection program, transmission by any means, but does not include installation on a computer before the computer is delivered to a user pursuant to first retail sale of the computer.

(11) WEB PAGE.—The term ''Web page'' means a location, with respect to the World Wide Web, that has a single Uniform Resource Locator or another

single location with respect to the Internet, as the Federal Trade Commission may prescribe.

SEC. 9. EFFECTIVE DATE AND SUNSET.

(a) EFFECTIVE DATE.—Except as specifically provided otherwise in this Act, this Act shall take effect upon the expiration of the 180-day period that begins on the date of the enactment of this Act.

(b) SUNSET.—This Act shall not apply after December 31, 2008.